CONGRESSIONAL TESTIMONY

[PLA Perspectives on Network Warfare in "Informationized Local Wars"]

Testimony before U.S.–China Economic and Security Review Commission

[February 17, 2022]

Dean Cheng

Senior Research Fellow for Chinese Political and Security Affairs,

The Heritage Foundation

My name is Dean Cheng. I am the Senior Research Fellow for Chinese Political and Security Affairs at The Heritage Foundation. The views I express in this testimony are my own, and should not be construed as representing any official position of The Heritage Foundation.

The People's Republic of China (PRC), including the Chinese People's Liberation Army (PLA) has not fought a war since 1979. However, the PLA has been a careful observer of other people's wars since at least the 1990s. By observing American wars, including the First Gulf War (1990), the invasion of Afghanistan (2001), and the Iraq War (2003); NATO's conflict in the Balkans (1990s); and Russian conflicts in Georgia (2008) and Syria, the PLA reached certain conclusions about the likely characteristics of any future wars it will be engaged in.

PLA Assessment of War in the Information Age

The most important is that victory or defeat in future wars will be a function of the ability to exploit information. Indeed, in the eyes of both the Chinese Communist Party as well as the PLA, as the world has entered the Information Age, the currency of international power, including economic and military capacity, is increasingly a function of the ability to harness information. The growing importance of information in the realm of defense is reflected in the evolution of the PLA's "military strategic guidelines (*junshi zhanlue fangzhen*; 军事战略方针)." These guidelines are the closest equivalent to the U.S. National Military Strategy, and provide guidance for PLA "force development, planning, and disposition."[1]

Since 1993, the PLA's military strategic guidelines have twice been modified; in each case, the modifications have reflected the growing role of information in future warfare. In 1993, the PLA was intent on preparing for "local wars under modern, high-technology conditions." This shifted to preparing for "local wars under informationized conditions" in 2004, and then to preparing to fight and win "informationized local wars" in 2015. In essence, the PLA has steadily sharpened its focus from high technology in general to information technology as the centerpiece of future warfighting capabilities.

[1] Joel Wuthnow, "What I Learned From the PLA's Latest Strategy Textbook," ***Jamestown Foundation China Brief*** (XXI, 11, May 25, 2021), https://jamestown.org/program/what-i-learned-from-the-plas-latest-strategy-textbook/

The rise of the Information Age, where the gathering, analysis, and exploitation of information has become essential, has seen the concomitant rise of "informationized warfare (*xinxihua zhanzheng*; 信息化战争)." This is defined as system-of-systems conflict involving the use of informationized weapons and associated tactics in the land, sea, air, outer space, and network and electronic spaces. It is marked by a reliance on networked information systems, and is viewed by the PLA as the basic form of warfare in the Information Age. [2]

This growing emphasis on information technology is in turn tied to the PLA's analysis of how future wars will be fought.

First, based on Chinese assessments of American, NATO, and Russian wars, the PLA deems it likely that its future wars will likely be *joint*. For the PLA, however, the concept of "jointness" has in turn steadily evolved from involving multiple different services operating in close physical proximity and at roughly the same time, to operations across multiple domains under a single command structure, in accordance with a single plan. The PLA's forces will need to interoperate in not only the traditional land, sea, and air domains, but also outer space and the electromagnetic domain.

To conduct joint operations successfully, however, it is essential that the participating forces in any future operations have the ability to *share information* and forge a *common situational awareness*. This in turn requires the ability to handle vast amounts of data, including from not only myriad military sensors (of all the services), but also local and national sources, which may include not only military but political, financial, and economic information. The PLA must be networked, not only among its component services and branches, but also with local and national infrastructure and governments. The integrated joint operations envisioned by the PLA therefore requires not only a single, unified command structure, but an integrated information network for sharing and fusing information from all sources and then distributing that information rapidly to all the participating forces across all the domains. As one Chinese author notes, "Future joint operations are built upon the foundation and with the support of networked informational systems-of-systems."[3]

At the same time, it is presumed that an adversary will be similarly networked, both within their military forces and to their broader respective local and national governments, infrastructure, and institutions. In particular, the United States is seen as being experienced with handling massive amounts of data and fielding a thoroughly networked military and broader economy. Those networks are therefore essential targets for the PLA and the broader Chinese network warfare community.

The ability to establish control of information and information flow at a particular time and within a particular space is the essence of establishing "information dominance (*zhi xinxi quan*; 制信息权)."[4] It entails the ability to collect more information, manage it faster, and employ it more precisely than the adversary.[5] The side that enjoys information dominance can then seize and retain the initiative, and force the adversary into a reactive mode, losing the ability to influence the outcome of an

[2] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 48.

[3] TANG Renjiang, "The More We Emphasize Jointness, the More We Must Push Regulation-Based Administration," *PLA Daily* (November 23, 2020) http://www.qstheory.cn/qshyjx/2020-11/23/c_1126773694.htm

[4] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 79.

[5] Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia,* 2nd Edition, *Military Strategy* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 68.

engagement. Information dominance is built upon both defending one's own networks and attacking and degrading the adversary's.

In light of the military strategic guidelines, and in support of the efforts to undertake joint operations and establish information dominance in future conflicts, the PLA has been undertaking an extensive, multi-faceted modernization program. The most visible element has been the steady improvement in the PLA's arsenal. From anti-ship ballistic missiles to domestically produced aircraft carriers to stealth fighters and light tanks, the current PLA has enjoyed a steady flow of new equipment over the past three decades, to the point that this is arguably the most well-equipped and sophisticated force ever fielded by the People's Republic of China.

As important, this modernization effort has included substantial acquisitions of platforms and systems that can help establish information dominance. In major PLA parades in 2009 and again in 2015, for example, the PLA Air Force fly-by was led by airborne early warning (AEW) aircraft.[6] The PLA has tested a variety of space weapons, including kinetic kill vehicles and now service satellites that can disrupt or destroy an adversary's satellites.[7]

PLA Reorganization

This equipment modernization was complemented on December 31, 2015, when the PLA underwent the most extensive reorganization since its founding. Almost every aspect of its structure was affected. The various measures are encapsulated in the Chinese statement, "The Central Military Commission manages the overall; the war zones are responsible for warfighting; the services are responsible for [military force] building (*junwei guanzong, zhanqu zhuzhan, junzhong zhujian；军委管总，战区主战，军种主建*)." Each aspect included elements to improve the ability of the PLA to undertake more informationized operations.

In terms of the *Central Military Commission* (CMC), the reorganization saw an expansion from the previous four general departments to fifteen departments, commissions, and offices.

Name	Chinese Name	Chinese characters
CMC General Office	Junwei bangong ting	军委办公厅
CMC Joint Staff Department	Junwei lianhe canmou bu	军委联合参谋部
CMC Political Work Department	Junwei zhengzhi gongzuo bu	军委政治工作部
CMC Logistics Support Department	Junwei houqin baozhang bu	军委后勤保障部
CMC Equipment Development Department	Junwei zhuangbei fazhan bu	军委装备发展部

[6] "Warplanes Fly Over Tianamen Square in Rehearsal," Xinhua (September 22, 2009) https://covid-19.chinadaily.com.cn/china/2009-09/22/content_8722768.htm and Alexander Neil, "China Parade to Display Past and Future," BBC (September 1, 2015) https://www.bbc.com/news/world-asia-34105252

[7] Brett Tingly, "A Chinese Satellite Just Grappled Another and Pulled It Out of Orbit," The Drive (January 27, 2022) https://www.thedrive.com/the-war-zone/44054/a-chinese-satellite-just-grappled-another-and-pulled-it-out-of-orbit

CMC Training and Management Department	Junwei xunlian guanli bu	军委训练管理部
CMC National Defense Mobilization Department	Junwei guofang dongyuan bu	军委国防动员部
CMC Discipline Inspection Commission	Junwei jilu jiancha weiyaun hui	军委记律检查委员会
CMC Politics and Law Commission	Junwei zhengfa weiyuan hui	军委政法委员会
CMC Science and Technology Commission	Junwei kexue jishu weiyuan hui	军委科学技术委员会
CMC Strategic Planning Office	Junwei zhanlue guihua bangongshi	军委战略规划办公室
CMC Reform and Organization Office	Junwei gaige he bianzhi bangongshi	军委改革和编制办公室
CMC International Military Cooperation Office	Junwei guoji junshi hezuo bangongshi	军委国际军事合作办公室
CMC Audit Office	Junwei shenjishu	军委审计署
CMC Office Affairs and General Administration	Junwei jiguan shiwu guanli zongju	军委机关事务管理总局

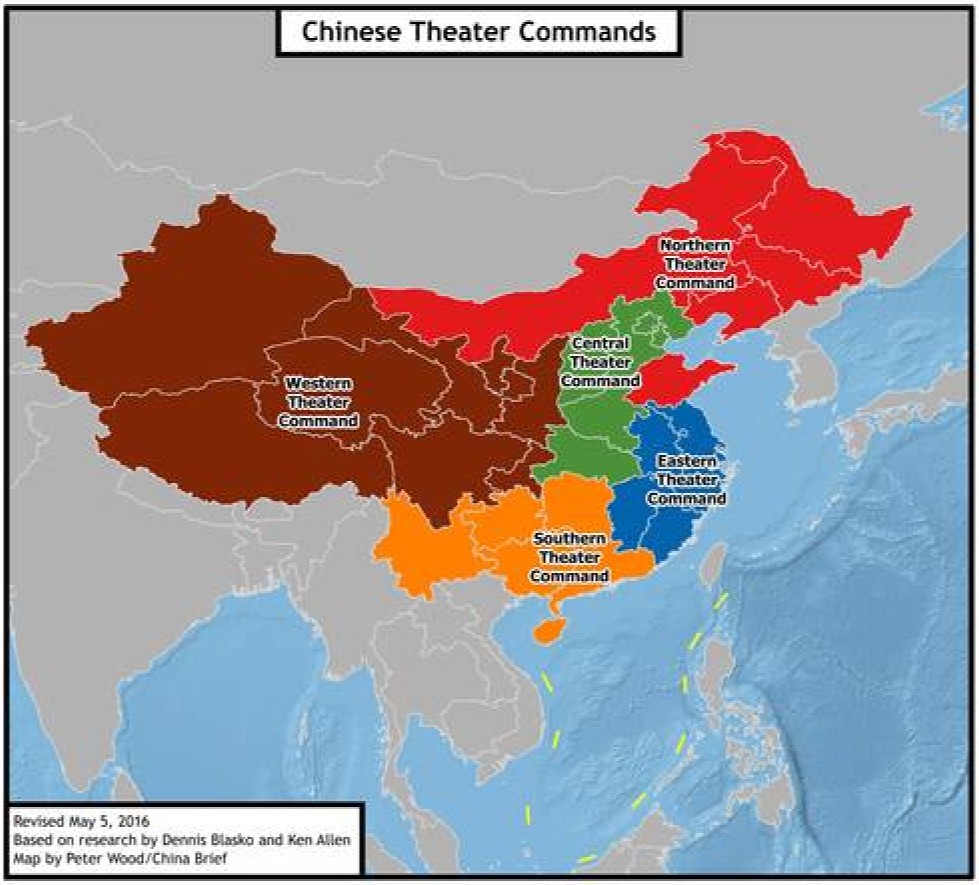
Notably, the previous General Staff Department, responsible for war planning and overall command of the PLA, has now become the CMC Joint Staff Department. This highlights the importance of joint operations in the PLA's vision of future conflicts, and underscores the need for PLA commanders to think in terms of the entire military and not just the ground forces (which had previously dominated the staffing of the CMC).

Meanwhile, the previous General Political Department (GPD) has had its functions divided among the CMC Political Work Department, the CMC Discipline Inspection Commission, and the CMC Politics and Law Commission. This would suggest that the new CMC Political Work Department will focus on such tasks as the conduct of political warfare (including the "three warfares" of public opinion warfare, psychological warfare, and legal warfare), while criminal and anti-corruption investigations (also previously a GPD responsibility) may now be the task of the CMC Discipline Inspection Commission. Political warfare is seen as an integral part of establishing information dominance.

The creation of some of the new departments and commissions also reflects the elevation of key areas to prominence. In particular, the establishment of the CMC National Defense Mobilization Department reflects the growing importance of not only mobilization planning for the PLA, but also the effort at integrating civilian and military efforts in a variety of areas. Chinese concepts of mobilization extend beyond mobilization of manpower and some industrial facilities to the ability to employ key infrastructure for military ends, and the mobilization of key personnel, equipment, and facilities to supplement military forces. This would be especially important in the context of "civil-military fusion" of information warfare resources, including Chinese telecoms, cyber security firms, and information technology industries.

In terms of the new *war zones* (or theaters or theater commands), the reorganization saw the PLA transition from seven military regions (MRs) to five war zones (WZs). These are:[8]

Name	Likely focus
Northern War Zone	Mongolia, Russia, Korean peninsula
Eastern War Zone	Taiwan, Japan, East China Sea
Southern War Zone	South China Sea, Southeast Asia
Western War Zone	India, South Asia, Central Asia, "counterterrorism" in Xinjiang and Tibet
Central War Zone	Strategic reserve, support to other war zones



[9]

Unlike the previous MRs, these WZs are headed by new, joint headquarters that are permanent establishments. This means that the associated staffs are regularly operating together, and would already be familiar with each other in event of war. As important, whereas all the MRs had always

[8] Office of the Secretary of Defense, ***Military and Security Developments Involving the People's Republic of China 2021*** (Washington, DC: Department of Defense, 2021), p. 97, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF

[9] http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=45069&no_cache=1#.V-FwUzVGRuo

been headed by ground force officers, several of the WZs are now headed by PLA Air Force and PLA Navy officers, emphasizing again the importance of joint operations.

Finally, the reorganization saw *the establishment of new services*, as well as the promotion of the Chinese nuclear forces from the Second Artillery "super-branch" to the PLA Rocket Forces. Relative to the goal of fighting "informationized local wars," a key organization is the new PLA Strategic Support Force (PLASSF). This entity brings China's space, network warfare, and electronic warfare forces under a single structure. The PLASSF's forces are responsible for achieving space dominance (*zhi tian quan;* 制天权), network dominance (*zhi wangluo quan;* 制网络权) and electronic dominance (*zhi dianzi quan;* 制电子权), which are in turn essential to establishing information dominance.

Notably, the PLASSF also incorporated Base 311 from the previous GPD. Base 311 was responsible for conducting political warfare, especially the "three warfares." "The 311 Base is the PLA's sole organization that is publicly known to focus on psychological warfare."[10] Political warfare, by influencing perceptions and assessments of military and political decision-makers, complements all other operations.

The PLASSF is very much the PLA's Information Warfare Force.

It is likely that there is a PLASSF contingent at each of the new WZ joint headquarters. This would be consistent with the presumption that future wars will entail cyber warfare, electronic warfare, and space warfare.

The PLASSF is especially noteworthy as it marks a truly innovative approach to the challenges of information warfare and modern conflict more broadly. The PRC is following a distinctly different path than either Russia or the United States. The Russian military, for example, established the Russian Aerospace Forces by combining the Russian Air Force and the Russian Aerospace Defense Force. Russian cyber forces do not appear to be part of the Russian Aerospace Forces.

Similarly, in the United States, there is no single service or combatant command that combines space, electronic warfare, and computer network warfare operations. Fielding of space forces is the responsibility of a new service, the United States Space Force (USSF), while the conduct of military space operations is the responsibility of US Space Command (USSPACECOM), a unified combatant command. Computer network operations are the responsibility of Cyber Command (USCYBERCOM), another unified combatant command, drawing upon the various services for cyber-capable forces. CYBERCOM shares some tasks with the National Security Agency, an intelligence organization and not a military force. Electronic warfare, meanwhile, is the responsibility of individual services.

Doctrinal Evolution

Alongside new equipment and a new organizational structure has been the promulgation of new doctrine. In November 2020, the PLA issued the "Chinese PLA Joint Operations Gangyao (Test)." (*zhongguo renmin jiefangjun lianhe zuozhan gangyao (shixing)*; 中国人民解放军联合作战纲要 [试行]) "Gangyao" (translated by the Chinese as "programs") are somewhat akin to field manuals, but have the authority of doctrine. They are a key part of the Chinese system of rules and regulations, helping to create a more standardized approach to various policy issues.[11] They also provide more specific

[10] John Costello and Joe McReynolds, ***China's Strategic Support Force: A Force for a New Era*** (Washington, DC: NDU Press, 2018), p. 17.

[11] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 569.

details, fleshing out the military strategic guidelines.[12] As with past military "gangyao," the PRC government has not released any version for public examination, but there has been significant discussion of these new ones.

According to PLA analyses, the sustained, ongoing development of information technologies, including artificial intelligence, big data, and cloud computing, have combined to create "new circumstances (*xin xingshi*; 新形势)" for military operations. The result has been essentially a military scientific revolution, requiring new operational forms and theories, and potentially further alterations of the PLA's organization.[13]

In particular, the development of these three technologies has opened a new stage in PLA thinking about the requirements for modernization. Where the PLA had long focused on becoming "fully mechanized and fully informationized," it now includes a new modernization goal of "intelligence-ization (*zhineng hua*; 智能化)."[14] The concept entails incorporating more artificial intelligence and machine learning into various platforms and systems. Building atop big data and cloud computing, the concept of "intelligence-ization" would seem to focus on allowing more data processing to occur within weapons and platforms, to better handle the huge amounts of data that are now flowing through the various networks.

These new "gangyao" apparently reflect these new circumstances. At a Chinese Ministry of Defense press conference, a PLA Defense Ministry spokesman observed that these new "gangyao" are necessary, both because of the PLA's reorganization and because of major changes in the global military situation. Thus, these new "gangyao" address the foremost issue: What kind of war will the PLA have to fight, and how will it fight that war?

According to the spokesman, the new "gangyao" provide more concrete guidance on how to conduct joint operations, especially in the face of new challenges and threats. Given the new organizations and structures within the PLA, these new "gangyao" are expected to clarify and strengthen the chain of command, including the relative roles of the CMC and the war zone command structures. As important, "it emphasizes the application of new types of combat strength."[15] The spokesman also notes that, in striving to meet the goal of a fully modernized PLA by 2027, the new "gangyao" will help the processes of mechanization, informationization, and intelligence-ization to be both accelerated and melded.

PLA Approach to Network Operations

Given the evolution of the PLA's view of the role of information in future wars, it is essential to note that the PLA's approach to information dominance does not appear to focus solely on cyber operations.

[12] Han Lin, Wei Bing, and Liu Jianwei, "Pushing Joint Operations Training to a Higher Level—'Chinese PLA Joint Operations Gangyao (Test)' Implementation After a Year," *PLA Daily* (January 5, 2022) http://www.mod.gov.cn/topnews/2022-01/05/content_4902340.htm

[13] FANG Xiaozhi, "These Five Years, What New Achievements have Chinese National Defense and Army-Building Reform Gained"? Overseas Network (December 29, 2018) https://k.sina.cn/article_3057540037_b63e5bc502000eb49.html

[14] XIAO Tianliang, Chief Editor, *Science of Military Strategy* (Beijing, PRC: National Defense University Press, 2020), p. 334, and PRC Ministry of Defense press conference transcript (November 26, 2020) http://www.mod.gov.cn/jzhzt/2020-11/26/content_4874643.htm

[15] PRC Ministry of Defense press conference transcript (November 26, 2020) http://www.mod.gov.cn/jzhzt/2020-11/26/content_4874643.htm

Indeed, it is important to recognize that the Chinese term "*wangluo zhan* (网络战)," while translated as "cyber war," is more accurately rendered as "network warfare."

Network warfare occurs in the realm of "network space (*wangluo kongjian*; 网络空间)," a term that roughly parallels that of "cyberspace." However, network warfare is seen as moving beyond just computer networks, although computer network warfare remains an integral element of network warfare. In relation to information warfare at the campaign level, it occurs within networks that are part of the overall battlefield (which can extend to outer space and deep into the two sides' homelands as part of the command and control, and logistical and support infrastructures).[16]

For the PLA, network warfare, also termed "network conflict (*wangluo duikang*; 网络对抗)," is comprised of the range of activities that occur within networked information space, as the two sides seek to reduce the effectiveness of the adversary's networks, while preserving one's own.[17] It includes not only offensive and defensive components, but also reconnaissance of adversary and others' networks.

The purpose of network warfare is to establish "network dominance (*zhi wangluo quan*; 制网络权)." When one has network dominance, the full range of one's own networks (not just computer networks) can operate smoothly and the information on those networks is safeguarded while being rapidly moved and applied; meanwhile an adversary's networks are prevented from doing the same. Some of the networks that are integral to network warfare include the command and control network, intelligence information network, and air defense network. [18] In Chinese writings, network space is sometimes described as the sixth domain (alongside land, sea, air, outer space, and the electromagnetic spectrum). In other cases, however, it is seen as the fifth domain, encompassing the electromagnetic spectrum.

Because of the importance of these various networks in the conduct of joint operations, informationized local wars will inevitably entail network warfare. For the weaker player, it is an especially potent means of neutralizing or weakening a stronger adversary's capabilities. One Chinese analysis observes that in the Balkan conflicts of the 1990s, although the Serbian forces were generally outmatched by NATO, they were nonetheless able to repeatedly penetrate various NATO networks and degrade their operations. The Chinese write that the Serbs were able to penetrate the networks of the aircraft carrier USS *Theodore Roosevelt* and British Meteorological Office, affecting air operations.[19] Another Chinese analysis similarly observes that the disparities in conventional strength between NATO and Serbia were not paralleled on the Internet, where Serbian forces successfully attacked various NATO and individual member states' web-sites.[20] Networks are so central to the

[16] YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 28.

[17] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 286, and YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 24.

[18] YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 24, 25.

[19] YUAN Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2009), p. 14.

[20] YUAN Wenxian, *The Science of Military Information* (Beijing, PRC: National Defense University Press, 2007), p. 73.

PLA's concept of modern warfare that one Chinese article suggests that informationized warfare is not possible without networks.[21]

While network warfare can yield powerful effects, PLA analysts seem to see it, and all other operations, as primarily embedded within a broader array of actions, as part of system-of-systems warfare (*tixi zuozhan*; 体系作战). Given the increasingly complex nature of modern warfare, individual platforms and even individual systems (*xitong*; 系统), by themselves, are unlikely to be decisive. Rather, conflicts are decided by the ability of rival arrays of systems, systems-of-systems (*tixi*; 体系), to out-perform each other.[22]

Systems-of-systems, in turn, are the product of integration through information flow. An effective information network allows information gathering, networking of forces and capabilities, and generation of synergies, to create a system-of-systems operational capacity that is substantially greater than what individual systems can bring to bear.[23] Success in future conflicts will therefore require all the various networks (information gathering, communications, command and control, weapons, logistics), drawn from all the participating services and operating across the various domains, to be able to work together, both in human as well as technical terms.[24]

Disrupting the adversary's networks, on the other hand, leads to the disintegration of their system-of-systems construct. This will significantly reduce their effectiveness, even if individual systems are able to function. Consequently, network warfare is an integral part of preserving one's own system-of-systems while degrading the adversary's.

An essential element of forging system-of-system effects is to integrate network and electronic warfare. This is the embodiment of the Chinese concept of unified joint operations. According to the PLA, electronic warfare, (*dianzi zhan*; 电子战), is the effort by each side to degrade and disrupt the adversary's electronic systems, while preserving one's own. [25] While electronic warfare is nominally aimed at equipment such as radars, communications systems, weapons control and guidance systems, and electronic countermeasures and electronic counter-countermeasures, it is actually about dominating the "electromagnetic space (*dianci kongjian*; 电磁空间)," or electromagnetic spectrum, ranging from super low frequencies to ultraviolet, including the visible light spectrum. [26]

Because electronics are now integrated into the very function of most weapons, electronic warfare now occupies a much more central role in establishing information dominance. Indeed, electronics have assumed a growing proportion of the cost and sophistication of modern weapons; some of the most expensive elements of modern warships and combat aircraft are the onboard electronics, rather than the metal. As one PLA analysis noted, electronics represent 20% of the cost of a modern warship,

[21] "How to Break Network 'Points' in System-of-Systems Operations," PLA Daily (May 2, 2017) http://military.people.com.cn/n1/2017/0502/c1011-29247744.html

[22] BAI Bangxi, JIANG Lijun, "Systems of Systems Conflict Is Not the Same as Systems Conflict," *National Defense Newspaper* (January 10, 2008).

[23] "How to Break Network 'Points' in System-of-Systems Operations," PLA Daily (May 2, 2017) http://military.people.com.cn/n1/2017/0502/c1011-29247744.html

[24] Li Yingming, Liu Xiaoli, et. al., "An Analysis of Integrated Joint Operations," *PLA Daily* (April 12, 2005)

[25] WANG Hui, *Foundational Knowledge, Considerations, and Explanations of Informationized Warfare* (Beijing, PRC: Military Science Publishing House, 2009), p. 180.

[26] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 255.

24% of the cost of a modern armored fighting vehicle, 33% of a military aircraft, 45% of a missile, and 66% of a satellite.[27]

As network warfare expands and electronic warfare systems are networked, the Chinese see network warfare and electronic warfare as inextricably linked. Indeed, Chinese military theorists were among the earliest adopters of the concept of "integrated network-electronic warfare (INEW)," and see INEW as a fundamental characteristic of information warfare and the informationized battlefield. [28]

The PLA defines the INEW concept (which it at times translates as "network-electronic integration warfare)" as a form of information warfare where one implements information attacks against the enemy's networked information systems through highly melded electronic warfare and network warfare."[29] It is those information warfare methods that use a combination of electronic warfare and network warfare techniques to attrit and disrupt the adversary's networked information systems, while defending one's own, in order to secure information dominance over the battlefield. For the PLA, INEW is the main expression of information warfare.[30]

As one Chinese analysis notes, in future conflicts, the electromagnetic spectrum will be the key influence upon the operation of network-space, with network and electronic warfare organically linked, operating under a single unified direction.[31] Therefore, network warfare will be affected by efforts aimed at dominating the electromagnetic spectrum, while the ability to operate electronic systems will be directly affected by efforts to penetrate and damage networks. The two elements are seen as mutually complementary in a unified effort to degrade the enemy's system-of-systems. Neither electronic warfare nor network warfare alone can comprehensively disrupt that system-of-systems, but given the mutually supporting nature of the two different types of warfare in terms of attack concepts, attack methods, and operating environments, they constitute a highly effective integrated attack methodology.

One Chinese volume observes:

> From a technical angle, electronic warfare and network warfare can be greatly complementary. Electronic warfare emphasizes attacking the signal layer, with the use of strong electromagnetic energy to drown out target signals. Network warfare emphasizes attacking the information layer, using disruptive information flow, transported into the enemy's network systems, as the means of attack.[32]

[27] WANG Hui, *Foundational Knowledge, Considerations, and Explanations of Informationized Warfare* (Beijing, PRC: Military Science Publishing House, 2009), p. 179.

[28] Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November, 2005), p. 101.

[29] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), pp. 262-263.

[30] Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia,* 2nd Edition, *Military Command* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 327.

[31] YE Zheng, *Concepts of Informationized Operations* (Beijing, PRC: Military Science Publishing House, 2007), p. 157 and YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 27.

[32] YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), pp. 28-29.

In the Chinese view, as individual facilities and their attendant information systems are networked together, the physical infrastructure upon which information passes and the information itself become an integrated whole. INEW is an effort to unify the concrete physical aspects and virtual aspects of information warfare, merging them into a single concept of operations.[33] By undertaking attacks on both of these elements, it is more likely that one can establish information dominance. INEW therefore envisions using electromagnetic attack and defense and information attack as the main techniques for degrading adversary ability to gather and exploit information, treating networked information systems as the domain of operations. Successful conduct of integrated network and electronic warfare should lead to dominance of the entire battlefield information space (*zhanchang xinxi kongjian*; 战场信息空间).

Notably, Chinese INEW targets include key parts of strategic command and control networks. According to one recent PLA textbook, key strike targets (*zhongdian daji mubiao*; 重点打击目标) for INEW include national and military decision-making elements, strategic early warning systems, military information networks, and financial, energy and transportation networks.[34]

The central point of the Chinese conception of INEW is the incorporation of targeting (and defense) of the ***physical element*** of the information networks into network warfare. This is what makes INEW more than simply adding electronic warfare techniques to network warfare; it expands information warfare beyond the predominantly virtual world of data to include the physical, tangible world. In the context of the greater emphasis on unified joint operations, INEW is envisioned as a key example of the new kind of unified jointness necessary to successfully fight informationized local wars.[35]

Indeed, alongside INEW is integrated network and firepower operations. Given the importance of the physical element of information networks, kinetically attacking key information and communications nodes, including server farms and command posts, can potentially disrupt information flow as much as corrupting the data or jamming transmitters and receivers.

Chinese Concepts of Information Deterrence

In addition to fighting and winning future "informationized local wars," the PLA, and the broader Chinese information and network warfare capacity, are charged with effecting deterrent strategies. As with actual conflict, the PRC's concept of deterrence is highly holistic. Beijing has been pursuing "multidomain deterrence" for many years, and information deterrence has long been one element of this broad approach.

According to Chinese analyses, the rapid advances in information technology coupled with globalization have wrought a fundamental shift in the world's socio-economic situation. We now live in the Information Age, with information being the primary currency of international power. "Outer space and information space and network and electromagnetic space have become the new main focal

[33] Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November, 2005), p. 101

[34] XIAO Tianliang, Chief Editor, *Science of Military Strategy* (Beijing, PRC: National Defense University Press, 2020), p. 235

[35] YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 28.

points for major powers interested in developing their economy and increasing their comprehensive national power. It has become the new 'high ground' for maintain security."[36]

The growing role of information and associated technologies has led to "information deterrence" becoming a new aspect of deterrence, or *weishe* (威慑). Just as information itself has become an instrument of conflict, the ability to threaten a nation's information systems directly affects societal stability, popular livelihood, and national survival.[37] According to Chinese analyses, "information deterrence" conceptually includes deterrence in the cyber realm, but goes further, encompassing all aspects of information and information operations.

"Information deterrence (*xinxi weishe*; 信息威慑)" is defined in the PLA's terminological reference volume as, "a type of information operations activity in which one compels the adversary to abandon their resistance or reduce the level of resistance, through the display of information advantage or the expression of deterrent/coercive information."[38] As with other PLA writings on deterrence, the Chinese approach to information deterrence does not differentiate between a coercive and a dissuasive effect.

The 2007 edition of the *PLA Encyclopedia* defines "information deterrence" as those activities in which "threats that employ information weapons or which implement information attacks against an opponent, lead to shock and awe and constrain the adversary."[39] Interestingly, this definition notes that "information deterrence" relies in part upon warning an adversary of the serious consequences of an attack (including through demonstration), creating fears that will influence the other side's cost-benefit analysis. The purpose of information deterrence, again, is to allow the deterring side to "achieve a particular political goal (*dadao yiding de zhengzhi mubiao*; 达到一定的政治目标)," ***not*** to prevent the other side from acting in the information domain.

Another Chinese study guide defines it as "a national display of information advantage or the ability to employ information operations to paralyze an adversary's information systems, so as to threaten that adversary. This serves to constrain the other side, as part of the deterrent/coercive goal."[40] What is clear across these various definitions is that "information deterrence," like the broader Chinese conception of deterrence in general, includes both dissuasion and coercion, and embodies the idea of deterring ***through*** information operations, rather than deterring operations ***in*** information space.

Chinese Information Deterrence Activities

From the Chinese perspective, the importance of information in the successful conduct of warfare means that one can also employ threats against the adversary's ability to obtain and exploit information

[36] XIE Xiang, *National Security Strategy Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 126.

[37] XIAO Tianliang, General Editor, *The Science of Strategy* (Beijing, PRC: National Defense University Publishing House, 2015), p. 123.

[38] All Army Military Terminology Management Committee, Academy of Military Sciences, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 262.

[39] Chinese People's Liberation Army National Defense University Scientific Research Department, *Chinese Military Encyclopedia*, 2nd Edition, *Military Strategy* (Beijing, PRC: Chinese Encyclopedia Publishing House, 2007), p. 283.

[40] AMS Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide—400 Questions about Informationized Operations* (Beijing, PRC: Military Science Publishing House, 2005), p. 15.

in order to deter and coerce them. Among states with roughly equivalent levels of information technology, given the widespread penetration of the Internet into all aspects of life, the potential ability to massively disrupt the adversary's entire society provides an opportunity to engage in deterrence. Indeed, on a day-to-day basis, Chinese writings suggest they believe that information deterrence is already in effect among equal players, precisely because the scale of disruption that would otherwise erupt would be enormous, while few states are confident of their ability to avoid such disruptions.[41]

However, where there is a distinct imbalance in information capabilities, it is harder for the weaker side to effect information deterrence. Conversely, the side that may be weaker in terms of conventional military power but who has significant network warfare capabilities may well be able to paralyze and disrupt the more conventionally capable side, and at least impose greater costs, if not actually defeat them.[42]

In the Chinese view, the ability to successfully conduct offensive information operations is therefore the most important means of implementing information deterrence. A demonstrated capability of exploiting information to one's own end, even if not employed, will nonetheless arouse concerns in the adversary. To this end, network offensive power, the ability to conduct effective computer network attack operations is essential, as it is seen as the foundation for information deterrence.[43]

This is in part because computer network attack (CNA) capabilities are relatively inexpensive, yet able to exploit a variety of means of attack, especially since computer networks now permeate so many aspects of society, the economy, and national security. Consequently, there is an unprecedented ability to employ CNA to paralyze and disrupt an adversary across much of its society. Moreover, there is a wide range of capabilities that can be employed, and a variety of vulnerabilities that can be exploited. These elements make network security difficult, both in terms of establishing counters but also establishing attribution.[44]

Consequently, the implicit threat underlying information deterrence is harder to counter than conventional, nuclear, or space deterrence. Indeed, the uncertainty confronting all states even now about the ultimate effect of information operations, and especially attacks against each other's information networks, is believed to be a major factor in forestalling the occurrence of large-scale network conflict.[45]

Chinese analysts seem to believe that this uncertainty creates the opportunity for robust information deterrence. In event of a crisis, PLA analysts suggest that one could remind an adversary of one's ability to plant computer viruses or otherwise undertake information attacks, in order to warn them to

[41] Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), p. 196.

[42] Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November, 2005), pp. 15-16.

[43] Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November, 2005), p. 15.

[44] XIAO Tianliang, General Editor, *The Science of Strategy* (Beijing, PRC: National Defense University Publishing House, 2015), p. 123.

[45] Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), p. 190.

cease and desist their resistance. At a minimum, such moves are considered likely to affect the adversary's will to fight.

At the same time, a clearly demonstrated ability to defend and safeguard one's information resources and systems can also serve to deter an adversary. If the adversary is unable to successfully attack one's information systems, then their ability to establish information dominance is likely to be extremely limited. In which case, their ability to establish dominance over other domains (e.g., air, space, maritime) is also likely to be very constrained, reducing their chances of successfully achieving whatever strategic objectives they might have. Under such circumstances, the adversary is likely to be deterred from initiating aggression, or may be coerced into submitting.

A Possible Information Deterrence Ladder

Given Chinese writings about deterrence activities in the space and nuclear domains, it is possible that there is a "deterrence ladder" for information operations. Chinese writings suggest such a construct is indeed being explored.[46] One article by a PLA expert from the Chinese military's Academy of Military Sciences lays out such a conceptual ladder for information deterrence.[47]

- *Deterrence through network technology experimentation* (*wangluo kongjian jishu shiyan weishe*; 网络空间技术试验威慑) The first, basic step for information deterrence is to undertake testing and development of new technologies associated with network warfare. This includes cyber weapons, but also new offensive methods and tactics. As important, one should allow such efforts to be revealed through the media, thereby informing the rest of the world of one's capabilities. A strong foundation in information technology and training is essential. As important, because of the rapid pace of development in this field, new breakthroughs may occur at any time; uncertainty about that can also support deterrent policies.
- *Deterrence through network equipment displays and demonstrations* (*wangluo kongjian zhuangbei zhanshi weishe*; 网络空间装备展示威慑) Where the first step of information deterrence is demonstrating technological capabilities, the second step involves demonstrating a broader array of network warfare capabilities, including equipment development plans, prototype testing, and equipment production. This approach will deliberately reveal to an adversary China's overall capabilities (rather than individual pieces of equipment or programs), as well as demonstrate that they are part of a broader, integrated development effort. Specific elements of this rung include the publication of white papers (such as the Chinese defense white paper), newspaper and magazine articles, and other official releases of information.
- *Deterrence through network operational exercises* (*wangluo kongjian zuozhan yanxi weishe*; 网络空间作战演习威慑). Simply displaying network capabilities, and discussing them, may not deter a potential adversary. The next rung on the Chinese information deterrence ladder is therefore to undertake operational exercises. This can involve forces deploying and operating in a real environment or a simulated one. The article suggests that public exercises involving forces in the field are typically defensive, while more offensive operations are undertaken in simulated environments, such as national cyber test ranges. The article specifically mentions the American "Schriever" space wargames as an example of how the United States displays and develops network warfare capabilities and signals its resolve to employ them.

[46] All references in this section, unless otherwise noted, are drawn from Yuan Yi, "AMS Expert Discloses Network Space Deterrence," China Military Web (January 6, 2016), http://news.xinhuanet.com/mil/2016-01/06/c_128599390.htm

[47] The People's Liberation Army Academy of Military Science is the leading brain trust for the PLA. It is comparable to a combination of the RAND Corporation, the US Army's Training and Doctrine Command (for the entire PLA), the Inspector General directorate, and some aspects of the Command and General Staff College (for the entire PLA).

- *Deterrence through actual network operations* (*wangluo kongjian zuozhan xingdong weishe*; 网络空间作战行动威慑). In both the nuclear and space contexts, the highest level of deterrent action is the actual employment of nuclear and space capabilities respectively, intended to signal an adversary the critical nature of the situation, and to demonstrate resolve. As important, employment of such weapons can affect the initial campaign, if the target is sufficiently valuable. This article suggests a similar mindset may exist for information deterrence, i.e., that the highest rung would be the employment of actual network warfare capabilities against an adversary's systems. This might involve a direct attack against key adversary networks, in order to preempt an enemy attack, or in response to an adversary's probe, as retaliation (and a demonstration of capability). The articles provided by the article suggest a more psychological focus, as they include disrupting email networks, generating a flood of text messages, and attacks against the power grid.

Interestingly, in the 2020 edition of the PLA National Defense University's *Science of Military Strategy*, network deterrence is described as primarily comprising strategic-level network deterrence (*zhanlue ji wangluo weishe*; 战略级网络威慑) and tactical-level network deterrence (*zhanshu ji wangluo weishe*; 战术级网络威慑).[48] The former is about displaying network offensive capabilities that could disrupt an adversary's key strategic networks, including political, economic, and military targets. Specific examples cited include the adversary's C4ISR networks, national transportation nodes, and national communications networks. By displaying the ability to strike an enemy's strategic targets, the expectation is that the enemy will be dissuaded from proceeding.

Tactical level network deterrence, on the other hand, is apparently primarily oriented towards discouraging criminals, hackers, and other lower-scale threats from operating, thereby maintaining the stability and operability of one's networks in peacetime.

It is important to keep in mind that in all these discussions, information deterrent activities are not occurring in isolation, but would be coordinated with a host of comparable activities in other domains and fields. These would involve not only military forces (e.g., naval exercises, space exercises), but also diplomatic and political pronouncements, economic measures, etc. This is especially likely to be the case at the higher rungs on the ladder.

At the same time, however, because China confronts a variety of potential adversaries, its leaders must constantly strive to engage in multilateral deterrence. Therefore, the Chinese leadership may not necessarily engage only in deterrent activities against, say, the United States or Japan, even in the midst of a crisis with those states. Heightened operations or limited offensive information operations, in the deterrent context, may be undertaken against third parties, both in order to demonstrate capability and resolve against the main target, but also to signal those third parties (and others) that China has sufficient capability to degrade them as well.

* * * * * * * * * * * * * * * * * * *

The Heritage Foundation is the most broadly supported think tank in the United States. During 2020, it had hundreds of thousands of individual, foundation, and corporate supporters representing every state in the U.S. Its 2020 operating income came from the following sources:

Individuals	66%
Foundations	18%
Corporations	2%

[48] XIAO Tianliang, Chief Editor, *Science of Military Strategy* (Beijing, PRC: National Defense University Press, 2020), p. 152.

Program revenue and other income 14%

The top five corporate givers provided The Heritage Foundation with 1% of its 2020 income. The Heritage Foundation's books are audited annually by the national accounting firm of RSM US, LLP.